



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 150  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/721,228	11/26/2003	Marco Sasselli	3829-020-27	9959

24510 7590 12/29/2006  
DLA PIPER US LLP  
ATTN: PATENT GROUP  
1200 NINETEENTH STREET, NW  
WASHINGTON, DC 20036

EXAMINER
----------

REZA. MOHAMMAD W

ART UNIT	PAPER NUMBER
----------	--------------

2136

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	12/29/2006	PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

**Office Action Summary**

Application No.

10/721,228

Applicant(s)

SASSELLI ET AL.

Examiner

Mohammad W. Reza

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 26 November 2003.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-14 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-14 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 26 November 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1:121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)            | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)   | Paper No(s)/Mail Date: _____                                      |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date <u>08/11/05</u> .  | 6) <input type="checkbox"/> Other: _____                          |

**DETAILED ACTION**

1. Claims 1-14 are presented for examination.

***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-14 are rejected under 35 U.S.C. 102(e) as being anticipated by James A, Sutton et al hereafter Sutton (US patent application 20030196096).

3. As per claim 1, Sutton discloses method characterized by following steps:

selection by means of the apparatus of a current key from a list of public keys, decryption of said block by the current public key, deactivation of the current key and selection of the next key in the list (paragraphs, 0021, 0027) reception and storage in the memory of the updating patch, reception of the encrypted control block, verification that the decrypted control block corresponds to said patch, installation of the patch received (paragraphs, 0013-0014, and 0026).

4. As per claim 2, Sutton discloses Method according to claim 1 wherein the control block includes a signature on the patch data, this signature being the result of a hash function (paragraphs, 0013-0014, and 0026).

Art Unit: 2136

5. As per claim 3, Sutton discloses method wherein the verification of the block includes the step of establishing the signature on the received patch and the comparison with the decrypted signature in the control block (paragraphs, 0030-0031).
6. As per claim 4, Sutton discloses method wherein the control block includes a symmetrical session key determined by the managing center, this key being used to encrypt the patch data (paragraphs, 0021, 0027).
7. As per claim 5-7, Sutton discloses method wherein, for each update, a new public key taken from the list is used by the apparatus, wherein the public key is deleted from the list after being used, said key being useless for the next updates, and wherein the public keys of the list are used sequentially in a predetermined order during each update (paragraphs, 0021, 0027).
8. As per claim 8, Sutton discloses method wherein the list of public keys is stored in a non-volatile memory, a key used for an update is definitively deleted from the memory that authorizes the access to the next key for the subsequent update (paragraphs, 0014).
9. As per claim 9, Sutton discloses method wherein, for the updating of the software of an apparatus of a certain version to a new version, with a difference between the new version and the previous one greater than one, at least one message encrypted with a private key is added allowing the changing of the current key to the next key in the list, the successful decryption of said message inducing the deactivation of the current key and the selection of the next key (paragraphs, 0021, 0027).

Art Unit: 2136

10. As per claim 10, Sutton discloses method wherein the number of messages corresponds to the number of updates separating the initial version of the apparatus and the final version of the update (paragraphs, 0013-0014, and 0026).

11. As per claim 11, Sutton discloses method wherein an updating installation is followed by an increment on a counter or by moving a pointer indicating the position of the key to be selected from the list during the subsequent update, while the list of keys remains unchanged (paragraphs, 0021, 0027).

12. As per claim 12, Sutton discloses method according to claim 1, wherein the control block is successively encrypted by the keys of the previous updates, each key from the list being used one after the other to decrypt the signature (paragraphs, 0030-0031).

13. As per claim 13, Sutton discloses method wherein the apparatuses consist of Pay-TV decoders, an update of a decoder being carried out by downloading, from a managing center, of a patch accompanied by a control block, said block is stored in a Random Access Memory, and is decrypted with a current public key contained in a first non-volatile memory of the decoder, then verified and in the case of correspondence, a command leads the installation of the patch in a second non-volatile memory and the deactivation of the current key (paragraphs, 0021, 0027).

14. As per claim 14, Sutton discloses method wherein a new list of public keys is transmitted to the decoder, said list replaces the list contained in the first memory containing keys deactivated by previous successful updates (paragraphs, 0021, 0027).

### ***Conclusion***

15. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mohammad w. Reza whose telephone number is 571-272-6590. The examiner can normally be reached on M-F (9:00-5:00).

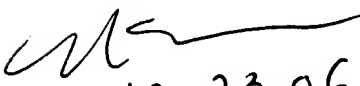
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, MOAZZAMI NASSER G can be reached on (571)272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Mohammad Wasim Reza

AU 2136

NASSER MOAZZAMI  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100

  
12/23/06